IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION

COMMUNITY PARTNERS GROUP, INC. Plaintiff, v. REGIONS BANK Defendant.	)	Case No. 2:24-cv-2581-JPM-tmp

ORDER GRANTING MOTION TO DISMISS

Before the Court is Defendant Regions Bank's ("Defendant's" or "Regions'") Motion to Dismiss Plaintiff Community Partners Group, Inc.'s ("Plaintiff's" or "CPG's") claims for damages and statutory interest under Alabama Code § 7-4A-101 et seq. (ECF No. 25.) Because Plaintiff has not pled sufficient facts to state its claims for relief, Defendant's Motion to Dismiss is **GRANTED**.

I. BACKGROUND[1]

A. Factual Background

Plaintiff is a Tennessee corporation which maintains various bank accounts with Defendant. (ECF No. 1-1 at PageID 10; ECF No. 25 at PageID 146.) One of these accounts is Plaintiff's account ending in 3520 (the "3520 Account"), which Plaintiff uses to process its payroll. (ECF No. 21 ¶ 9.) The Master Agreement for Treasury Management Services (the "Agreement") governs the 3520 Account. (ECF No. 25 at PageID 146; ECF No. 21 ¶ 9.)

[1] For purposes of the Motion to Dismiss, the Court takes the facts alleged in the Complaint as true. See Ashcroft v. Iqbal, 556 U.S. 662, 666 (2009). This section should not be construed as a finding on any listed fact.

At approximately 2:30 p.m. on July 3, 2023, Plaintiff became aware of an automated clearing house ("ACH") credit transaction (the "ACH Transaction") on the 3520 Account. (ECF No. 21 ¶¶ 10, 12.)[2] The ACH Transaction payment details (the "Payment Details") show four separate payments from the 3520 Account, done via Defendant's iTreasury ACH service,[3] to Henechka Natallia, Ivan Yaneko, and Mariia Shevtsova (collectively, "Russian hackers"), for a total of $82,458.55. (See ECF No. 25 at PageID 149; ECF No. 25-1 at PageID 160.) The Payment Details show user AFISHER entered and approved the ACH Transaction between 12:41 and 12:50 p.m. on July 3, 2023. (See ECF No. 25-1 at PageID 160.) The user AFISHER corresponds to Amy Fisher, Plaintiff's treasurer. (See ECF No. 21 ¶ 19.) The ACH Transaction was perpetrated by these Russian hackers. (Id. ¶ 11.)

Plaintiff's president, Allen Fisher, then went to a local Regions branch to attempt to stop the ACH Transaction. (Id. ¶¶ 12–17.) However, the branch manager did not do so because she believed it was from the IRS. (Id. ¶ 15.) An employee of Defendant then assured Allen Fisher the money would not be released from Plaintiff's account. (Id. ¶ 17.) On July 5, 2023, however, Defendant processed the ACH Transaction. (Id. ¶ 21.) Plaintiff has yet to recover $58,095.30 of the funds. (Id. ¶ 22.)

B. Procedural Background

Plaintiff filed its original Complaint in the Circuit Court of Shelby County, Tennessee for the Thirtieth Judicial District at Memphis on July 3, 2024, and served Defendant with a summons and copy of the Complaint on July 16, 2024. (ECF No. 1 ¶¶ 1–2.) Defendant removed

[2] Although Plaintiff alleges the transaction was a debit, the Court analyzes it as an ACH credit transaction because Plaintiff's cause of action derives from an instruction from Plaintiff's account to pay a different account. (See Ala. Code § 7-4A-104 cmt. 4; ECF No. 25 at PageID 149 n.2.)

[3] Defendant's iTreasury service allows Customer to "review account transactions and information and perform certain transactions and banking services via the Internet." (ECF No. 28 at PageID 207.)

the case to this Court on August 15, 2024. (Id.) The Court has diversity jurisdiction over the Parties under 28 U.S.C. § 1332. (ECF No. 21 ¶ 3.)

Plaintiff originally asserted claims for breach of contract, negligence, a violation of Tennessee Code Annotated § 47-4-101 et seq., punitive damages, and attorneys' fees. (ECF No. 1-1 ¶¶ 20–41.) After a Scheduling Conference with the Court, however, Plaintiff agreed Alabama law governed the dispute. (ECF No. 20 at PageID 88 n.1.) Plaintiff filed its Amended Complaint, the operative complaint here, on October 1, 2024. (See ECF No. 21.) In its Amended Complaint, Plaintiff asserts: (1) a claim for damages under Alabama Code § 7-4A-101 et seq.; and (2) a claim for statutory interest under Alabama Code §§ 7-4A-204, 7-4A-506. (Id. ¶¶ 25–44.)

Defendant filed the instant Motion on October 29, 2024. (ECF No. 25.) The Motion was fully briefed on December 10, 2024. (See ECF Nos. 27 (Response, Nov. 26, 2024), 29 (Reply, Dec. 10, 2024).)

II. LEGAL STANDARD

A. Failure to State a Claim

Federal Rule of Civil Procedure 12(b)(6) allows dismissal of a complaint that "fail[s] to state a claim upon which relief can be granted." It permits the "defendant to test whether, as a matter of law, the plaintiff is entitled to legal relief even if everything alleged in the complaint is true." Mayer v. Mylod, 988 F.2d 635, 638 (6th Cir. 1993) (citing Nishiyama v. Dickson Cnty., 814 F.2d 277, 279 (6th Cir. 1987)). A motion to dismiss allows the Court to dispose of meritless cases which would waste judicial resources and result in unnecessary discovery. Brown v. City of Memphis, 440 F. Supp. 2d 868, 872 (W.D. Tenn. 2006).

When evaluating a 12(b)(6) motion, the Court must determine whether the complaint alleges "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (citing Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). A claim is plausible on its face if "the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. (citing Twombly, 550 U.S. at 556).

A complaint need not contain detailed factual allegations. Twombly, 550 U.S. at 570. A plaintiff without facts who is "armed with nothing more than conclusions," however, cannot "unlock the doors of discovery." Iqbal, 556 U.S. at 678–79; Green v. Mut. of Omaha Ins. Co., No. 2:10-2487-SHM-tmp, 2011 WL 112735, at *3 (W.D. Tenn. Jan. 13, 2011), aff'd, 481 F. App'x 252 (6th Cir. 2012). A court "need not accept as true legal conclusions or unwarranted factual inferences." Morgan v. Church's Fried Chicken, 829 F.2d 10, 12 (6th Cir. 1987). "While legal conclusions can provide the framework of a complaint, they must be supported by factual allegations." Iqbal, 556 U.S. at 679.

B. Credit Transfers Under Alabama Law

The issuance and acceptance of credit transfers is governed by Alabama Code § 7-4A-201 et seq. Plaintiff's claim arises under § 7-4A-204(a), which states:

> If a receiving bank accepts a payment order issued in the name of its customer as sender which is (i) not authorized and not effective as the order of the customer under Section 7-4A-202, or (ii) not enforceable, in whole or in part, against the customer under Section 7-4A-203, the bank shall refund any payment of the payment order received from the customer to the extent the bank is not entitled to enforce payment and shall pay interest on the refundable amount calculated from the date the bank received payment to the date of the refund.

Thus, the Court examines whether the ACH Transaction was (1) authorized or effective under § 7-4A-202; and (2) enforceable under § 7-4A-203. See Ala. Code § 7-4A-204(a). Both

prongs are necessary conditions to grant Defendant's Motion to Dismiss. See id. If Plaintiff has pled sufficient facts such that either prong is not satisfied, Defendant's Motion will be denied. See id.

III. ANALYSIS

The Court first examines what evidence to consider at this stage of litigation. Second, the Court analyzes whether the ACH Transaction was authorized or effective under § 7-4A-202. Third, the Court analyzes whether the ACH Transaction was enforceable under § 7-4A-203. Finally, the Court considers Plaintiff's claim for statutory interest under §§ 7-4A-204, 7-4A-506.

A. Evidence to Consider

At the motion to dismiss stage, "a court may consider 'exhibits attached [to the complaint], public records, items appearing in the record of the case[,] and exhibits attached to [a] defendant's motion to dismiss so long as they are referred to in the [C]omplaint and are central to the claims contained therein,' without converting a motion under 12(b)(6) into one for summary judgment." Rondigo, LLC v. Twp. of Richmond, 641 F.3d 673, 681 (6th Cir. 2011) (quoting Bassett v. Nat'l Collegiate Athletic Ass'n, 528 F.3d 426, 430 (6th Cir. 2008) (changes in original)).

However, "[t]his does not include [a] plaintiff['s] responses to a motion to dismiss." Waskul v. Washtenaw Cnty. Cmty. Mental Health, 979 F.3d 426, 440 (6th Cir. 2020) (citation omitted). A plaintiff "cannot 'amend their complaint in an opposition brief or ask the court to consider new allegations (or evidence) not contained in the complaint.'" Id. (quotation omitted).

Plaintiff attached five documents with its Amended Complaint. (See ECF Nos. 21-1 (3520 Account Contract), 21-2 (The Agreement), 21-3 (IRS Correspondence), 21-4 (Counsel Correspondence), 21-5 (Regions Letter).) The Court considers each of these documents as

necessary. See Com. Money Ctr., Inc. v. Ill. Union Ins. Co., 508 F.3d 327, 335 (6th Cir. 2007) ("documents attached to the pleadings become part of the pleadings and may be considered on a motion to dismiss"). The Court also considers the Payment Details because they are attached to the instant Motion and are central to the claim, (see ECF No. 25-1). See Snodgrass-King Pediatric Dental Assocs., P.C. v. DentaQuest USA Ins. Co., 79 F. Supp. 3d 753, 761 (M.D. Tenn. 2015).

The Court, however, will not consider Plaintiff's new arguments and documents included with its Response. (See ECF Nos. 27, 27-1.) In its Response, Plaintiff argues the Agreement is unenforceable because it is a contract of adhesion and unconscionable. (ECF No. 27 at PageID 169.) However, nowhere in its Amended Complaint does Plaintiff make either assertion. (Cf. ECF No. 21.) Thus, the Court will not consider Plaintiff's new allegation that the Agreement is a contract of adhesion or unconscionable.[4] See Waskul, 979 F.3d at 440. Similarly, the Court will not consider Plaintiff's argument that the laptop used to access the 3520 Account was not hacked because it relies on an exhibit attached to the Response, (see ECF No. 29-1), and is not raised in the Amended Complaint, (cf. ECF No. 21). See Waskul, 979 F.3d at 440.

B. Authorization and Effectiveness

The Court now analyzes whether the ACH Transaction was authorized or effective as the order of Plaintiff under § 7-4A-202. See Ala. Code § 7-4A-204(a)(2)(i).

Because Plaintiff has alleged Russian hackers perpetrated the transaction, (ECF No. 21 ¶ 11), the Court can draw a "reasonable inference" Plaintiff did not "authorize the [ACH Transaction] or is otherwise bound by it under the law of agency." See Ashcroft v. Iqbal, 556

[4] Even if the Court were to consider whether the Agreement is a contract of adhesion or unconscionable, these arguments are unavailing because (1) Plaintiff is not a consumer such that contract of adhesion analysis would apply, see Ex parte United Propane, 258 So. 3d 1103, 1109 (Ala. 2018); and (2) Plaintiff has not shown it lacked meaningful alternatives such that the Agreement is a contract of adhesion, see id., or unconscionable, Briarcliff Nursing Home, Inc. v. Turcotte, 894 So. 2d 661, 667 (Ala. 2004).

U.S. at 678; Ala. Code § 7-4A-202(a). Thus, Plaintiff has pled sufficient facts the ACH Transaction was not authorized. See Ala. Code § 7-4A-202(a). Thus, the Court only examines whether the ACH Transaction was effective. See id.

For this, the Court looks to § 7-4A-202(b), which states:

> If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and (ii) the bank proves that it accepted the payment order in good faith and in compliance with the bank's obligations under the security procedure and any agreement or instruction of the customer, evidenced by a record, restricting acceptance of payment orders issued in the name of the customer.

Ala. Code § 7-4A-202(b). Thus, to determine whether the ACH Transaction was effective, the Court examines if (1) Defendant had a security procedure in place; (2) Defendant's security procedure was commercially reasonable; and (3) Defendant proved it acted in good faith and in compliance with its security procedure. See id. For the reasons enumerated below, the Court finds Plaintiff has not pled sufficient facts to show the ACH Transaction was not effective.

i. Defendant's Security Procedure

A security procedure is "a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication." Ala. Code § 7-4A-201.

The Court finds Defendant has a security procedure within the meaning of the statutory definition. The Agreement enumerates security procedures for a variety of services, including iTreasury ACH, which the ACH Transaction falls under. (ECF No. 28 at PageID 200, 208; see ECF No. 25-1.) It then defines any security procedure between the Parties as "any process or procedure . . . for the purpose of verifying that communications, orders, instructions, or inquiries

regarding a Service transaction or other Service activity are those of [the] [c]ustomer." (ECF No. 28 at PageID 183.) This falls squarely within § 7-4A-201(i).

ii. Commercial Reasonability of Defendant's Security Procedure

Defendant argues the ACH Transaction was authorized.[5] (See ECF No. 25 at PageID 153.) Defendant's arguments center around the text of the Agreement. Defendant first argues the Agreement states that Defendant's security procedures are "commercially reasonable." (See id. at PageID 152–53 (quoting ECF No. 28 at PageID 184).) Next, Defendant argues any transaction initiated through the 3520 Account is deemed effective regardless of whether Plaintiff authorized the ACH Transaction. (Id. at PageID 153 (citing ECF No. 28 at PageID 200).) Finally, Defendant argues Plaintiff is responsible for its data being compromised, with the Agreement stating, "[Plaintiff] agrees that [Defendant] is not responsible for any losses, injuries, or harm incurred by [Plaintiff] as a result of any electronic, e-mail, or internet fraud." (See id. (citing ECF No. 28 at PageID 185).)

Plaintiff disagrees and argues the ACH Transaction was not authorized.[6] (ECF No. 27 at PageID 171.) Plaintiff first argues commercial reasonability of Defendant's security procedures is a matter that requires further factual development. (Id. at PageID 172.) Plaintiff then argues it reported the ACH Transaction to Defendant in a timely manner. (Id.)[7]

[5] Defendant centers its argument around whether the ACH Transaction was authorized, citing Alabama Code § 7-4A-204(b) as the relevant portion of the statute. (See ECF No. 25 at PageID 152.) That subsection, however, focuses on effectiveness, not authorization. See Ala. Code § 7-4A-204(b) ("a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if . . ."). Thus, the Court considers these arguments in its analysis as to whether the ACH Transaction was effective. See id.

[6] Plaintiff similarly does not address effectiveness, only authorization. (See ECF No. 27 at PageID 171–173.) The Court considers these arguments in its analysis as to whether the ACH Transaction was effective, as it has already found the ACH Transaction was not authorized. (See supra n.5; supra Section III.B.)

[7] Plaintiff also argues (1) the contract is an unconscionable contract of adhesion and (2) it was Defendant, not Plaintiff, who could have been hacked. (See ECF No. 27 at PageID 171–72.) However, the Court will not consider these arguments nor the attachments which supposedly supports them. See supra Section III.A.

The Court finds Defendant's arguments persuasive. First, Plaintiff and Defendant agree Defendant's security procedures were commercially reasonable. (See ECF No. 28 at PageID 184 ("[Plaintiff] acknowledges and agrees that the Security Procedures, including (without limitation) any Security Devices used in connection therewith, constitute commercially reasonable security procedures under applicable law for the transactions and activity [Plaintiff] intends to effect through the Service").)

Second, the Agreement states:

> [Plaintiff] acknowledges and agrees that [Plaintiff] shall be bound by any and all transactions and activity effected through the Service through the use of such Security Procedures, whether authorized or unauthorized, and by any and all transactions and activity otherwise initiated by Authorized Users, to the fullest extent allowed by law.

(Id.) This alone deems Defendant's security procedures commercially reasonable, as "[Plaintiff] expressly agreed in a record to be bound by any payment order, whether or not authorized, issued in its name, and accepted by the bank in compliance with the bank's obligations under the security procedure chosen by the customer." See Ala. Code § 7-4A-202(c)(ii).

Furthermore, Plaintiff's reporting of the ACH Transaction is not relevant. See Ala. Code § 7-4A-202(b). Indeed, "[t]he effect of Section [7-]4A-202(b) is to place the risk of loss on the customer if an unauthorized payment order is accepted by the receiving bank after verification by the bank in compliance with a commercially reasonable security procedure." Ala. Code § 7-4A-203 cmt. 5.[8]

The commercial reasonability of Defendant's security measures therefore does not need further factual development. See Ala. Code § 7-4A-203 cmt. 4 ("The issue of whether a particular security procedure is commercially reasonable is a question of law."). Thus, § 7-4A-202(b)(ii) is satisfied.

[8] The official comments for § 7-4A-202 are covered in the comments for § 7-4A-203.

iii. Compliance with Security Procedure and Good Faith

As to its compliance with the security procedure and good faith inquiries, Defendant points to the Payment Details, arguing "[r]eceipt by Regions of the approvals necessary to satisfy the [P]arties' agreed security procedure under the [P]arties' Agreement establishes authorization for purposes of the statute." (See ECF No. 25 at PageID 149, 154; ECF No. 25-1.) Plaintiff, however, argues it is Defendant's burden to prove it acted in compliance and good faith, which is a factual question inappropriate at the motion to dismiss stage. (ECF No. 27 at PageID 173.)

Plaintiff's argument as to the factual nature of these inquiries is unavailing. While it is true Defendant's compliance with any security procedure is generally a question of fact, see Ala. Code § 7-4A-203 cmt. 4, here the Court need only determine if the ACH Transaction was "accompanied by [Plaintiff's] designated Security Devices." (ECF No. 28 at PageID 208.) If so, Defendant was authorized to perform the ACH Transaction under the agreed-upon security procedures. (See id. (describing the security procedures for the iTreasury ACH service).) This contract language is "clear and unambiguous" such that there is "no issue of fact to be determined." Richards v. Vanderbilt Univ., No. 3:08-CV-0161, 2009 WL 10728583, at *6 (M.D. Tenn. Jan. 5, 2009) (quoting Lincoln Elec. Co. v. St. Paul Fire & Marine Ins. Co., 210 F.3d 672, 684 (6th Cir. 2000)).

The Court finds Defendant complied with its security procedure. The username AFISHER and the ACH Company ID, both present in the Payment Details, (ECF No. 25-1), are "security devices" under the Agreement because they are "credentials" and "method[s] of authentication or identification used in connection with a [s]ecurity [p]rocedure." (ECF No. 28 at PageID 183.) Because the ACH Transaction was accompanied by security devices, Defendant

shows it complied with its security procedures in executing the ACH Transaction. (See id. at PageID 208.)

Regarding the factual nature of Defendant's good faith in executing the ACH Transaction, Plaintiff's argument is again unavailing. The Court here examines if Defendant "substantially complie[d] with the terms, conditions, and provisions set forth in [the] Agreement" when processing the ACH Transaction. (See id. at PageID 187.) If Defendant did so, then it "shall be deemed to have exercised ordinary care and good faith." (See id.)

The Court finds Defendant did substantially comply with the terms of the Agreement. Under the Agreement,

> initiation of a transaction using applicable Security Procedures constitutes sufficient authorization for [Defendant] to execute such transaction notwithstanding any particular signature requirements identified on any signature card or other documents relating to [Plaintiff's] Account, and [Plaintiff] agrees and intends that the submission of transaction orders and instructions using the Security Procedures shall be considered the same as [Plaintiff's] written signature in authorizing [Defendant]to execute such transaction.

(ECF No. 28 at PageID 184.) As detailed above, Defendant was authorized to process the ACH Transaction. Plaintiff only alleges Defendant has not complied with the Agreement regarding the ACH Transaction. (Cf. ECF No. 21.) Because Defendant substantially complied with the terms of the Agreement regarding the ACH Transaction in that it was authorized, Plaintiff has not pled sufficient facts to show Defendant did not act in good faith. (See ECF No. 28 at PageID 187.)

C. Enforceability

The Court now analyzes whether the ACH Transaction was not enforceable, in whole or in part, against Plaintiff under § 7-4A-203. See Ala. Code § 7-4A-204(a)(2)(ii).

Section 7-4A-203(a)(2)(ii)[9] states:

[9] The Court only considers § 7-4A-203(a)(2)(ii) because the ACH Transaction was perpetrated by Russian hackers, (ECF No. 21 ¶ 12), and therefore was not "caused . . . by a person entrusted at any time with duties to act for [Plaintiff]." See Ala. Code § 7-4A-203(a)(2)(i).

> The receiving bank is not entitled to enforce or retain payment of the payment order if the customer proves that the order was not caused, directly or indirectly, by a person . . . who obtained access to transmitting facilities of the customer or who obtained, from a source controlled by the customer and without authority of the receiving bank, information facilitating breach of the security procedure, regardless of how the information was obtained or whether the customer was at fault.

Simply stated, "[i]f [Plaintiff] can prove that [the Russian hackers] committing the fraud did not obtain the confidential information from an agent or former agent of [Plaintiff] or from a source controlled by [Plaintiff], the loss is shifted to [Defendant]." See Ala. Code § 7-4A-204 cmt 5.

Defendant argues the ACH Transaction is enforceable because Plaintiff cannot "prove that these 'effective' transactions were not caused, directly or indirectly, by a person who obtained access to Plaintiff's banking information thus facilitating a breach of the security procedures." (ECF No. 25 at PageID 155–56 (citing Ala. Code § 7-4A-203(a)(2)(ii).)

Plaintiff counters the ACH Transaction is unenforceable because "the hackers herein obtained access to Plaintiff's Account by breaching Defendant's systems and/or equipment." (See ECF No. 27 at PageID 174.)

The Court finds Plaintiff has not pled sufficient facts to show the ACH Transaction was unenforceable. The mere allegation by Plaintiff that the ACH Transaction was "perpetrated by Russian hackers," (see ECF No. 21 ¶ 12), does not allow the Court to draw a "reasonable inference" that "the person committing the fraud did not obtain the confidential information from an agent or former agent of [Plaintiff] or from a source controlled by [Plaintiff]." See Iqbal, 556 U.S. at 678; Ala. Code § 7-4A-204 cmt 5.

Instead, the Court finds the Payment Details "trump[] the allegations" in the Amended Complaint. See Kreipke v. Wayne State Univ., 807 F.3d 768, 782 (6th Cir. 2015). The Payment Details show the ACH Transaction was entered and approved by user AFISHER. (See ECF No.

29-1.) Because Amy Fisher's account is a "source controlled by [Plaintiff]," Plaintiff has not pled sufficient facts to shift the loss to Defendant. See Ala. Code § 7-4A-204 cmt 5. Thus, Plaintiff still bears the risk of loss. See id. ("The effect of Section 4A-202(b) is to place the risk of loss on the customer if an unauthorized payment order is accepted by the receiving bank after verification by the bank in compliance with a commercially reasonable security procedure. An exception to this result is provided by Section 4A-203(a)(2).").

Plaintiff may argue the hackers only obtained access to its account by breaching its or Defendant's systems. To the extent the Court does consider this argument, (see supra Section III.A), it is unavailing. It does not matter "how the information was obtained or whether [Plaintiff] was at fault." See Ala. Code § 7-4A-203. The sole matter is whether the confidential information was obtained by a source controlled by Plaintiff, or a source controlled by the bank. See Ala. Code § 7-4A-203 cmt. 5. Because the confidential information was obtained from a source controlled by Plaintiff, Plaintiff has not pled sufficient facts to shift the loss to Defendant. See Ala. Code § 7-4A-204 cmt 5.

D. Statutory Damages

Plaintiff asserts a claim for statutory damages under §§ 7-4A-204, 7-4A-506. (See ECF No. 21 ¶¶ 39–44.) A receiving bank is required to pay interest on any payment order that is refundable—that is, either not authorized and not effective or not enforceable. See Ala. Code § 7-4A-204. Here, however, Plaintiff has not stated sufficient facts to show the ACH Transaction is refundable. See supra Sections III.B, III.C. Thus, Plaintiff has failed to state a claim for statutory interest. See Ala. Code § 7-4A-204.

IV. CONCLUSION

For the reasons discussed above, Defendant's Motion to Dismiss is **GRANTED**. Plaintiff's case is **DISMISSED WITH PREJUDICE**.[10]

SO ORDERED, this the 3rd day of March, 2025.

/s/ Jon P. McCalla
JON P. MCCALLA
UNITED STATES DISTRICT COURT JUDGE

[10] The Court dismisses the case with prejudice because Plaintiff has not sought leave to amend its Amended Complaint based on the current Motion, "despite ample opportunity to do so." See Ohio Police & Fire Pension Fund v. Standard & Poor's Fin. Servs. LLC, 700 F.3d 829, 844 (6th Cir. 2012). Thus, Plaintiff is bound by the default rule: "'if a party does not file a motion to amend or a proposed amended complaint' in the district court, 'it is not an abuse of discretion for the district court to dismiss the claims with prejudice.'" Id. (quoting CNH Am. LLC v. UAW, 645 F.3d 785, 795 (6th Cir. 2011)).